Privacy Year in Review: Recent Changes in the Law of Biometrics

MARGARET BETZEL*

ABSTRACT

Biometrics is a science that utilizes a person's physical characteristics to identify that person. Biometrics was thought of as merely science fiction, but now it is growing to be a part of everyday life. The law has had to change rapidly to keep up with the growing technology. This article addresses four major areas of biometrics and the legal implications involved, including: (1) facial recognition technology and camera surveillance, (2) regulation of those who enter the United States through biometric identifiers, (3) smart cards and national ID cards, and (4) DNA Databases.

I. INTRODUCTION

Biometrics came to the forefront of people's imaginations with George Orwell's *1984*. He created a world where cameras watched your every move and heard your every word.[1] However, the field of biometrics was created long before the world of *1984*. It began with Alphonse Bertillon, chief of the criminal identification division for the Paris police department. Bertillon used anthropometry, or the use of different body sizes and proportions, to identify criminals in the mid-nineteenth century.[2] Bertillon's method lost popularity, however, when fingerprints began to be used in the late nineteenth century.[3] Fingerprints have been an invaluable tool in criminal investigations ever since. Even though biometrics has historically been used in the

---

* Margaret Betzel is a candidate for juris doctor at The Ohio State University Moritz College of Law, class of 2006. She holds a bachelor's degree in zoology and chemistry from Miami University of Ohio.

[1] GEORGE ORWELL, 1984 (Penguin Books Ltd. 1950) (1949).

[2] *Anthropometry*, WIKIPEDIA (2005), at http://en.wikipedia.org/wiki/Anthropometry (last visited Apr. 3, 2005).

[3] Anil K. Jain, Salil Prabhakar, & Arun Ross, *An Introduction to Biometric Recognition* (appeared in 14 IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY: SPECIAL ISSUE ON IMAGE-AND VIDEO-BASED BIOMETRICS, 4 (2004), *available at* http://biometrics.cse.msu.edu/JainRossPrabhakarCSVT_v15.pdf (last visited Apr. 27, 2005).

criminal setting, biometrics today is increasingly being used in everyday life.

A. WHAT IS BIOMETRICS?

Biometrics involves techniques used to identify individuals based on a particular trait or physical characteristic unique to that individual.[4] Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

> *Universality*: each person should have the characteristic;
>
> *Distinctiveness*: any two persons should be sufficiently different in terms of the characteristic;
>
> *Permanence*: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;
>
> *Collectability*: the characteristic can be measured quantitatively.[5]

B. THE TWO FUNCTIONING MODES OF BIOMETRICS SYSTEMS: VERIFICATION MODE AND IDENTIFICATION MODE

A biometric system is "a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database."[6] These systems acquire and use biometric information in four steps: (1) a physical characteristic is scanned, (2) the characteristic is converted into digital code, (3) the code is stored in a database, and (4) the database and digital code are

---

[4] Lisa Jane McGuire, Comment, *Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up You Privacy*, 33 AKRON L. REV. 441, 444 (2000).

[5] Jain, *supra* note 3, at 1-2.

[6] *Id.* at 2.

accessed to identify the individual at a later time.[7] Biometrics systems can operate in two modes: a verification mode or an identification mode.

In verification mode, the biometric system validates a person's identity by comparing the person's biometric data with the stored biometric data previously collected and stored in the system database.[8] Common non-biometric verification mode systems include the use of a PIN number, a user name, or a password.[9] For example, when a person enters a password to log on to his or her computer, the computer conducts a one-to-one comparison to determine whether the claimed user is the correct person. The verification mode is usually used for *positive recognition*, where the goal is to prevent multiple people from using the same identity.[10]

In general, systems that operate in verification mode are successful and function well.[11] However, verification systems can make two types of errors: mistaking biometric measurements from two different persons to be from the same person (called a false match) and mistaking two biometrics measurements from the same person to be from two different persons (called a false non-match).[12] These errors in identification can be caused by a variety of factors, including imperfect imaging conditions (for example, with the use of a finger scanner, there could be sensor noise or dry fingers), changes in the user's physiological or behavioral characteristics (for example, cuts and bruises on the finger), ambient conditions (for example, changes in temperature and humidity), and the user's interaction with the sensor (for example, finger placement).[13]

---

[7] Robert H. Thornburg, Comment, *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment*, 20 J. MARSHALL J. COMPUTER & INFO. L. 321, 323 (2002).

[8] Jain, *supra* note 3, at 2.

[9] *Id.*

[10] *Id.*

[11] BROMBA, BIOMETRICS FREQUENTLY ASKED QUESTIONS, *at* http://www.bromba.com/faq/biofaqe.htm#Biometrie (last visited April 27, 2005).

[12] Jain, *supra* note 3, at 5.

[13] *Id.* at 4-5.

In every verification system, there is a trade-off between the false match rate and the false non-match rate.[14] If a system's sensitivity threshold is increased to allow for fewer false matches, then there will be more false non-matches. If a system's sensitivity threshold is lowered to allow for fewer false non-matches, then there will be more false matches.

A biometric system that functions in identification mode recognizes a person by searching all the users in the database for a match.[15] In this case, the system conducts a one-to-many comparison to establish a person's identity.[16] The identification mode is generally used for *negative recognition*, where the goal is to prevent a person from using multiple identities.[17] Unlike systems that function in verification mode, which can use non-biometric data to meet its goals, negative recognition can only be established through systems that use biometric data.[18]

C. WHAT TECHNOLOGIES DOES BIOMETRICS COVER AND WHAT ARE THE STRENGTHS AND WEAKNESSES OF EACH?

There are many technologies encompassed within biometrics. Each system has its own strengths and weaknesses. The choice of which system to use depends upon its application. A biometrics system is assessed through a variety of factors, including: recognition accuracy, speed, resource requirements, effect on users (the biometrics system should be relatively harmless), acceptability by the intended population, and resistance to various fraudulent methods and attacks to the system.[19] Below, is a brief discussion of the most commonly-used systems and their strengths and weaknesses.

> *Face*: Facial images are the most commonly used biometric characteristic.[20] Many people present a photo ID of

---

[14] *Id.* at 5.

[15] *Id.* at 2.

[16] *Id.*

[17] Jain, *supra* note 3, at 2.

[18] *Id.*

[19] *Id.*

[20] *Id.* at 8.

themselves almost daily. However, there now exist biometric systems that can verify that you match your picture. These systems are often limited because they require a fixed and simple background or special illumination.[21] They also have difficulty with identification if the image of the face is taken from a drastically different viewpoint than the stored image.[22] There is also a question as to whether the face provides a sufficient basis for recognizing a large number of identities.[23] Faces change throughout the aging process or can be altered using contacts, makeup, or even a different hairstyle.[24]

Signature: It is commonly accepted that a person's signature is unique to them. Signatures have been accepted as a biometric identifier in government, legal, and commercial transactions as a method of identification.[25] However, signatures are a behavioral biometric and may change over a period of time, as well as be influenced by physical and emotional changes in the person.[26] Professional forgers may also be able to reproduce signatures that fool biometric systems.[27]

Fingerprint: Fingerprint identification is very commonly used because of its accuracy in identifying an individual.[28] Fingerprint scanners are also highly affordable (the cost is approximately $20 when ordered in large quantities).[29]

---

[21] *Id.* at 9.

[22] Jain, *supra* note 3, at 9.

[23] *Id.*

[24] Gwen Kennedy, *Thumbs Up For Biometric Authentication!*, 8 COMP. L. REV. & TECH. J. 379, 386-387 (2004).

[25] Jain, *supra* note 3, at 11.

[26] *Id.*

[27] *Id.*

[28] *Id.* at 9.

[29] *Id.*

However, the fingerprint is not a perfect identifier. A fraction of the population is simply unsuitable for this type of identification. Genetic factors, aging, environmental, or occupational reasons (for example, the fingers of manual labor workers have a large number of cuts and bruises on them that may continually change their fingerprints) can make matching the person's fingerprints nearly impossible.[30]

DNA: Deoxyribonucleic Acid (DNA) is found in the nucleus of every person's cells. It is unique to each person, with the exception of identical twins who share the same DNA. DNA is commonly used in forensic applications for person recognition.[31] There are three potential problems with the use of DNA: 1. Contamination and sensitivity: It is easy to steal a person's DNA and use it to implicate that person.[32] Furthermore, DNA samples are easily contaminated at the laboratory level because some of the laboratory technicians' DNA can get into the sample during processing. 2. Automatic Real-time Recognition Issues: Assessing a DNA sample is cumbersome, time-consuming, and requires expertise.[33] 3. Privacy Issues: Information about susceptibilities of a person to certain diseases could be gained from the DNA sample. Because there is concern that abuse of this information could lead to "genetic discrimination," many are reluctant to expand the use of DNA as an identifier.[34]

Keystroke: There is a theory that every person types on a keyboard in a distinct way.[35] Keystrokes could be monitored

---

[30] Jain, *supra* note 3, at 9.

[31] *Id.* at 8.

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] Jain, *supra* note 3, at 8.

> unobtrusively; however, it is a behavioral biometric and may change over time.[36]
>
> *Iris*: The iris is the colored region of the eye. Its visual texture is formed during fetal development and becomes permanent by age two.[37] The iris is generally very complex and distinctive for identification purposes (the iris is even different in identical twins).[38] It is rather easy for an identification system to detect artificial irises.[39] Early iris systems were expensive and difficult to operate; however, the newer systems are more affordable and user-friendly.[40] Currently, iris scans are generally limited to high-end security applications.[41]

The field of biometrics is progressing rapidly. The remainder of this paper will discuss changes in the field of biometrics over the past 4 years and the legal problems that these technologies have encountered. There are four major places where the use of biometrics has overlapped with the law: (1) the fields of facial recognition technology and camera surveillance (2) regulation of those who enter the United States (3) smart cards, and (4) the use of DNA databases.

II. FACIAL RECOGNITION TECHNOLOGY AND CAMERA SURVEILLANCE

George Orwell said it best when he penned, "there was of course no way of knowing whether you were being watched at any given moment."[42] In Manhattan in 1998, volunteers counted 2,400 cameras in public places used to catch red-light runners on the road, shoplifters,

---

[36] *Id.*

[37] *Id.* at 10.

[38] *Id.*

[39] *Id.*

[40] Jain, *supra* note 3, at 10.

[41] Kennedy, *supra* note 24, at 385.

[42] ORWELL, *supra* note 1, at 2.

and drug sellers loitering near lampposts.[43] Today, there is biometric facial recognition technology that can match the recorded face to a database.[44] Even though this technology, and the potential for future technologies, may seem intrusive, there is little constraint on public surveillance.

A. CAMERA SURVEILLANCE AND THE FOURTH AMENDMENT

Many legal scholars argue that there is a right to anonymity under the Fourth Amendment and that video surveillance should be under strict control.[45] The courts have disagreed.[46] The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[47] In a Fourth Amendment analysis, one must first demonstrate that a person has a subjective expectation of privacy.[48] Next, that expectation must be shown to be reasonable.[49]

The Fourth Amendment has protected against unwanted surveillance within the home.[50] However, videotaping in public places has been upheld under the Fourth Amendment.[51] But, the courts have

---

[43] Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 214 (2002).

[44] Roberto Iraolo, *Lights! Camera! Action! - Surveillance Cameras, Facial Recognitions Systems, and the Constitution*, 49 LOY. L. REV. 773 (2003).

[45] *See* Slobogin, *supra* note 43; Iraolo, *supra* note 44.

[46] *See* United States v. Knotts, 460 U.S. 276 (1983); *but see* Slobogin, *supra* note 43.

[47] U.S.CONST. amend. IV.

[48] Thornburg, *supra* note 7, at 339.

[49] *Id.*

[50] *See* Payton v. United States, 445 U.S. 573, 590 (1971).

[51] *See* Sponick v. City of Detroit Police Department, 211 N.W.2d 674, 690 (Mich. Ct. App. 1973) in which the court held that a tavern was a public place and videotaping suspect did not violate fourth amendment.

recognized that there can be zones of privacy created in public places.[52]

In 2003, the Second Circuit Court of Appeals held that the use of a hidden camera worn by an informant was not an unreasonable search, and therefore, there was no violation of the Fourth Amendment.[53]

A case decided by the Ninth Circuit Court of Appeals in 2002 upheld the use of a hidden camera worn by a television reporter to obtain information about a business on the business's premises.[54] The Court found that because the manager of the business invited the disguised reporter onto the premises and voluntarily gave her a tour, the manager and the business did not have an objectively reasonable expectation to solitude or seclusion.[55] The Court also noted that the manager's conversations with the reporter were not protected because they merely discussed the operations of the company.[56] Only the privacy of individuals is protected, not the privacy of corporations.[57]

In 2004, courts endorsed the wide use of video surveillance. The Third Circuit Court of Appeals held that the use of cameras hidden in a hotel room to capture a defendant's bribery transactions was not a violation of the Fourth Amendment because the informant, who was also videotaped and participated in the sting operation, consented to the taping.[58] The court relied on *Lopez v. United States*,[59] in which the

---

[52] *See* Britt v. Superior Court of Santa Clara County, 374 P.2d 817 (Cal. 1962) in which the court held that videotaping criminal through a peephole into a public restroom was a violation of the Fourth Amendment. The court stated, "Man's constitutionally protected right of personal privacy not only abides with him while he is the householder within his own castle but cloaks him when as a member of the public he is temporarily occupying a room -- including a toilet stall -- to the extent that it is offered to the public for private, however transient, individual use. " Britt, 374 P.2d at 819. *See also* Ward v. State, 636 So. 2d 68 (Fla. Dist. Ct. App. 1994) in which the court held that officers peeking into a public restroom through a crack was a violation of the Fourth Amendment.

[53] United States v. Davis, 326 F.3d 361 (2d Cir. 2003).

[54] Medical Laboratory Management Consultants v. American Broadcasting Companies, 306 F.3d 806 (9th Cir. 2002).

[55] *Id.* at 813; *But see,* United States v. Taketa, 923 F.2d 665 (9th Cir. 1991) in which the court held that a defendant had a legitimate expectation of privacy in his office because it was available for his exclusive use during working hours and that the use of a hidden camera to tape his activities was a violation of the Fourth Amendment.

[56] *Id.* at 814.

[57] *Id.*

[58] United States v. Lee, 359 F.3d 194 (3d Cir. 2004).

Court held that "if a person consents to the presence at a meeting of another person who is willing to reveal what occurred, the Fourth Amendment permits the government to obtain and use the best available proof of what the latter person could have testified about."[60] The Third Circuit noted that the defendant had an expectation of privacy in the hotel room when he was there alone.[61] However, once he admitted the informant into the room, this expectation of privacy disappeared.[62] Furthermore, the court noted that there was no difference between an informant wearing the camera (which has previously been upheld) and the placement of the camera in a hotel room.[63] Therefore, there was no violation of the Fourth Amendment.[64]

B. CAMERA SURVEILLANCE AND STATE LAW

Camera surveillance has also been associated with state law during the year of 2004.

The California Court of Appeals upheld a state statute requiring certain cybercafe owners to implement video surveillance to prevent crime.[65]

The Louisiana Court of Appeals held that a self-storage company was contractually obligated to provide video surveillance because it had signs posted that said "Smile you are being videotaped."[66]

Finally, the Ohio Court of Appeals ruled this year that a video conference was sufficient to satisfy the confrontation clause for a defendant during a parole hearing.[67] Every criminal defendant has a

---

[59] Lopez v. United States, 373 U.S. 427 (1963).

[60] *Lee*, 359 F.3d at 200 (referencing *Lopez*, 373 U.S. at 439).

[61] *Id.* at 201.

[62] *Id.*

[63] *Id.* at 202.

[64] For contrasting authority, see United States v. Nerber, 222 F.3d 597 (9th Cir. 2000) in which the court held that video-tape that was recorded when the informants were not present in the hotel room should be suppressed because the defendants had a legitimate expectation to be free from surveillance.

[65] Vo v. City of Garden Grove, 115 Cal. App. 4th 425 (Cal. Ct. App. 2004).

[66] Allstate Ins. Co. v. Soulant Bros., No. 2003 2817, 2004 La. App. LEXIS 3128 (La. Ct. App. Dec. 17, 2004).

[67] Wilkins v. Wilkinson, 157 Ohio App. 3d 209 (Ohio Ct. App. 2004).

constitutional right to confront his witnesses.[68] The court found "that the use of videoconferencing technology permitted free and unimpeded visual and auditory communication"[69] which was sufficient to satisfy the confrontation clause.

C. FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology is a computer enhanced video surveillance system. This technology has developed into a security measure used to scan crowds and pick out known terrorists and criminals.[70] The system uses two components: video cameras to acquire the image of a person's face, and computer software to analyze that face for identification purposes.[71]

This system was used at the 2001 Super Bowl at Tampa's Raymond James Stadium.[72] It has also been implemented in Tampa's Ybor City entertainment district and the hockey arena of the Salt Lake City Winter Olympics.[73] In both locations, the use of the technology was discontinued due to its ineffectiveness.[74] Facial recognition technology is currently being installed in airports around the country to protect against terrorist attacks.[75] To date, there has never been a successful implementation of the technology and there has never been a terrorist or wanted criminal arrested through these systems.[76] However, it is still seen as the wave of the future.[77]

---

[68] *Id.* at 212.

[69] *Id.* at 215.

[70] Thornburg, *supra* note 7, at 321.

[71] *Id.* at 325.

[72] *Id.* at 321.

[73] *Id.*

[74] *Id.*

[75] Thornburg, *supra* note 7, at 322. In January of 2002, both the Fresno International Airport and St. Petersberg-Clearwater International Airport installed facial recognition systems. Shortly thereafter, the systems were installed in Dallas/Fort Worth, Boston Logan, and Palm Beach International Airports.

[76] *Id.* at 321.

[77] *Id.*

Some privacy advocates argue that facial recognition systems may violate the Fourth Amendment. As previously stated, in a Fourth Amendment analysis, one must first demonstrate that a person has a subjective expectation of privacy.[78] Next, that expectation must be shown to be reasonable.[79] Although people typically do not have a subjective expectation of privacy with regard to their face, if they put on a hat or sunglasses, this may show that they have an expectation of privacy.[80] Furthermore, it is possible to argue that just because a person goes to the grocery store does not necessarily show sufficient evidence of a lower expectation of privacy in his or her image.[81] As far as addressing the reasonableness inquiry, some argue that some uses of facial recognition technology may be *per se* unreasonable.[82] If the technology progresses to the point where it can track a person's day-to-day activities, it may be unreasonable and therefore violate the Fourth Amendment.[83]

III. REGULATION OF THOSE WHO ENTER THE UNITED STATES

Since September 11, 2001, there has been a dramatic increase in public concern about who is allowed to enter and live in the United States. In response, the federal government has implemented many new laws and procedures. For example, commercial pilots are now able to carry handguns and federal air marshals fly on many domestic flights to prevent the threat of a terrorist attack.[84] The new protections also incorporate biometrics.

---

[78] *Id.* at 339.

[79] *Id.*

[80] Thornburg, *supra* note 7, at 345.

[81] *Id.*

[82] *Id.* at 346.

[83] *Id.*

[84] Eric P. Haas, Comment, *Back to the Future? The Use of Biometrics. Its Impact on Airport Security, and How This Technology Should Be Governed*, 69 J. AIR L. & COM. 459 (2004).

A. US-VISIT

1. WHAT IS US-VISIT? A STATUTORY DESCRIPTION

The United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT) began on January 12, 2004.[85] This program was implemented by the Department of Homeland Security (DHS) as a response to several Congressional mandates that required the Department to

> create an integrated, automated entry exit system that records the arrival and departure of aliens; that equipment be deployed at all ports of entry to allow for the verification of aliens' identities and the authentication of their travel documents through the comparison of biometric identifiers; and that the entry exit system record alien arrival and departure information from these biometrically authenticated documents.[86]

Under this program, visitors that enter the United States from certain countries at select ports of entry will be photographed and fingerprinted by Customs officials.[87] These visitors must also "check out" when they leave through particular ports of entry.[88] The data collected is stored in the automated identification system (IDENT)[89] and will only be accessible by government officials.[90]

US-VISIT will initially only apply to "covered individuals," defined as people who are "nonimmigrant visa holders traveling through air and sea ports."[91] However, DHS does anticipate

---

[85] *Id.* at 479.

[86] Implementation of the United States Visitor and Immigrant Status Indicator Technology Program, 69 Fed. Reg. 468, 468 (Jan, 5, 2004) (to be codified at 8 C.F.R. pts. 214, 215, and 235).

[87] Haas, *supra* note 84, at 479.

[88] Implementation of the United States Visitor and Immigrant Status Indicator Technology Program, 69 Fed. Reg. at 473.

[89] *Id.* at 468.

[90] Haas, *supra* note 84, at 479.

[91] *Id.*

expanding the program to "eventually have the capability to verify the identities of most foreign national travelers through biometric comparisons."[92]

DHS has stated that it chose the collection of two fingerprints and photographs because they are less intrusive than other forms of biometric collections.[93] However, the Department has stated that it may expand what is collected based upon necessity and improved technology.[94] If a fingerprint cannot be obtained from an alien, the alien may provide another biometric identifier.[95] However, when the person's identity is not at issue and the alien cannot provide a fingerprint, the requirement may be waived.[96]

The department implemented this program through a series of amendments to regulations including, 8 C.F.R. § 235.1(d),[97] 8 C.F.R.

---

[92] Implementation of the United States Visitor and Immigrant Status Indicator Technology Program, 69 Fed. Reg. at 470.

[93] *Id.* at 471.

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] Implementation of the United States Visitor and Immigrant Status Indicator Technology Program, 69 Fed. Reg. at 470. This amendment allows DHS to require aliens who are arriving at United States air and sea ports to provide photographs, fingerprints, or other biometric identifiers. The amendment also provides that DHS will collect photographs and fingerprints from aliens applying for nonimmigrant visa upon their arrival at United States air and sea ports and upon departure.

§ 235.1(d)(ii),[98] 8 C.F.R. § 214.1(a),[99] 8 C.F.R. § 235.1(f),[100] as well as enacting 8 C.F.R. § 215.8.[101]

2. Is US-VISIT a Good Idea? Criticisms of the Program

US-VISIT has many supporters and many critics. Supporters frame arguments around the threat of a terrorist attack due to lax immigration laws, while critics worry about its impact on freedom and privacy.

US-VISIT could potentially violate the Fourth Amendment's protection of unwarranted search. However, the Supreme Court's decision in *United States v. Verdugo-Uquidez*[102] indicates that a program only limited to "nonimmigrant visa holders traveling through air and sea ports" will probably not fall within the protections of the Fourth Amendment.[103] In *Verdugo-Uquidez*, the Court found that the Fourth Amendment only protected "the people" being defined only to include "a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of the community."[104] The Court also noted that "the Bill of Rights is a futile authority for the alien seeking admission

---

[98] *Id.* This amendment states that if an alien refuses to provide the requested biometrics necessary to verify his identity and to authenticate travel documents, that alien may be inadmissible to the United States under section 212(a)(7) of the INA for lack of proper documents.

[99] *Id.* This amendment states that if a nonimmigrant alien is required to provide biometric identifiers, the alien's admission is conditioned on compliance with any such requirements. Also, if the alien is required to provide biometric information upon departure, his failure to comply may constitute a failure of the alien to maintain the terms of his immigration status.

[100] *Id.* This amendment states that all nonimmigrant aliens will be issued the Form I-94, Arrival Departure Record. These forms must be surrendered upon departure unless the I-94 was issued for multiple entries.

[101] *Id.* This new regulation states that the Secretary of Homeland Security may establish pilot programs at up to fifteen air or sea ports, through which the Secretary can require aliens who are leaving the United States to provide photographs, fingerprints, or other biometric identifiers and documentation to determine the alien's identity and whether he has properly maintained his status while in the United States.

[102] United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

[103] Haas, *supra* note 84, at 479.

[104] *Verdugo-Urquidez*, 494 U.S. at 265.

for the first time to these shores."[105] Because the Court has interpreted the protections of the Fourth Amendment narrowly, and as long as US-VISIT applies to a limited class of covered individuals, this program should not constitute an unwarranted and unreasonable search.[106]

Critics of US-VISIT have also expressed concern "over the cost, the lack of technological sophistication required for such a system, privacy loss possibilities, increases in racial profiling, and....loopholes in the system."[107]

Researcher Richard Sobel has stated, "the government would do much better using resources to better identify people [sic] and deter people who might cause some harm than to use resources devoted to the 99 percent of people who are innocent."[108]

Other critics argue that visitors from twenty-eight nations, including those nations whose citizens are not required to get visas for short stays in the United States, will not be scanned, leaving the United States just as open to terrorism.[109] Supporters of US-VISIT say that exempt countries are those that will require biometric information on their passports and that provides a sufficient safeguard.[110]

Critics are also concerned the methodology of the system. The search for every alien will require the system to perform an identification search of one fingerprint to millions of records of fingerprints.[111] This presents the opportunity for false positives and false negatives.

---

[105] *Id.* at 271 (citing Kwong Hai Chew v. Colding, 344 U.S. 590, 569 (1953)).

[106] Haas, *supra* note 84, at 480.

[107] Sarah McIntosh, Comment, *Developments in the Executive Branch: Department of Homeland Security Begins to Implement New US-VISIT Program*, 18 GEO. IMMIGR. L.J. 433, 434 (2004).

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] Frank Moss, *Changing the Face of Immigration: A Year in Transition*, 19 ST. JOHN'S J.L. COMM. 41, 42 (2004) (transcription of comments made at the St. John's Journal of Legal Commentary Symposium on Feb. 27, 2004).

B. MEXICAN BORDER-CROSSING CARD PROGRAM

Recently, a new program was implemented for Mexican citizens who work in the United States, but it has received little attention.[112] Under the old system, a Mexican citizen crossing the United States border to work for the day had to stand in a long line to present a visa or a passport. However, under this new program, if a Mexican citizen presents a Border-Crossing Card, containing a machine-readable biometric identifier, then he or she will be able to bypass the long line and the visa application process.[113]

IV. SMART CARDS AND NATIONAL ID CARDS

A. WHAT IS A SMART CARD?

A smart card is a card that is embedded with either a memory chip with non-programmable logic or a memory chip and a microprocessor.[114] A card with a microprocessor can add, delete, and manipulate information.[115] A memory-chip only card, such as a pre-paid phone card, can only perform predefined operations.[116] Smart cards differ from standard magnetic strip cards in that the smart card carries all necessary functions and information on the card.[117] In contrast, standard magnetic strip cards must have access to a database at the time of the transaction to work.[118]

B. HONG KONG'S NATIONAL ID CARDS

In October of 2000, the Hong Kong Special Administrative Region announced their plan to replace government-issued ID cards with

---

[112] 8 C.F.R. § 212.1(c)(2) (2005).

[113] *Id.*

[114] SUN MICROSYSTEMS, DOCUMENTATION: SMART CARD OVERVIEW, *at* http://java.sun.com/products/javacard/smartcards.html (last visited Apr. 27, 2005).

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Id.*

smart identity cards.[119] In Hong Kong, it is mandatory for every person above the age of 15 to register with the government, carry "proof of identity," and produce this proof of identity when requested.[120] The cards have the same basic data as a traditional ID card such as name, date of birth, and immigration status.[121] However, the card also stores unprecedented amounts of data, such as a digital photograph of the cardholder and an algorithm of the cardholder's thumbprints.[122] The Hong Kong government ID card has multiple uses, from storing information regarding immigration status to use as a library card.[123] The Hong Kong government plans to expand the uses of the smart card. These new uses include automatic voter registration and a machine-scannable passport to go in and out of mainland China.[124]

C. SMART CARDS IN THE UNITED STATES

Although, smart cards have been widely used in Europe and Asia, they are not as widely used in the United States.[125] The use of smart cards in the United States is usually in a business setting or, as seen more prominently, with travel.

1. IN AIRPORTS: THE TRUSTED TRAVELER SYSTEM

Smart Cards are already extensively used by airport employees to control access to restricted airport areas.[126] These cards contain

---

[119] Rina C.Y. Chung, *Hong Kong's "Smart" Identity Card: Data Privacy Issues and Implications for a Post-September 11th America*, 4 ASIAN-PACIFIC L. & POL'Y J. 442, 445 (2003).

[120] *Id.* at 451-452. This is mandated by the Registration of Persons Ordinance. H.K. Registration of Persons Ordinance ch. 177. Formally, this law required persons to card a standard government issued ID, but now it will require persons to carry the newly issued smart cards.

[121] *Id.* at 445.

[122] *Id.* at 446.

[123] *Id.* at 461.

[124] Chung, *supra* note 119, at 462-463.

[125] *Id.* at 443-444.

[126] Haas, *supra* note 84, at 481.

biometric components of the airport employees.[127] However, it has been suggested that biometric smart cards be required of the general traveler population.

US-VISIT, as previously discussed, currently only applies to "covered individuals," or those people defined as "nonimmigrant visa holders traveling through air and sea ports." However, government officials have already recommended modifying the program to aid in airport security. The most recent proposal is called "Trusted Traveler."[128] Initially, this program would be conducted on a volunteer basis.[129] The volunteers would agree to a background check and would then receive a card as a "trusted traveler."[130] The card would be a smart card that is made secure with biometric identifiers such as fingerprints or an iris scan.[131] The government claims that the "Trusted Traveler" system would increase airport security while decreasing the amount of time that travelers would have to spend at security check points.[132]

2. THE POTENTIAL FOR A UNIVERSAL SMART CARD SYSTEM

Many scholars believe that the United States will have some sort of universal smart card system in the near future. According to Richard Sobel, "[e]ven before the attacks on New York City and Washington, D.C. on September 11, 2001, America was moving toward a system of national identification numbers, databanks, and identity cards."[133] Sobel claims that a national identification system was created by five different statutory provisions: (1) The Immigration Reform and Control Act of 1986 ("IRCA"),[134] (2) The Illegal Immigration Reform

---

[127] *Id.*

[128] *Id.* at 480.

[129] *Id.*

[130] *Id.*

[131] Haas, *supra* note 84, at 480-481.

[132] *Id.* at 481.

[133] Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 HARV. J. LAW & TECH. 319, 320 (2002) [hereinafter Sobel, *Demeaning*].

[134] Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, 100 Stat. 3359 (1986). This statute required that employers have employees fill out and sign an I-9 verification form

and Immigrant Responsibility Act of 1996 ("IIRIRA"),[135] (3) The Personal Responsibility and Work Opportunity Reconciliation Act of 1996 ("Welform Reform Act"),[136] (4) The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[137] and (5) The Federal Aviation Administration ID requirement and Computer Assisted Passenger Screening System ("CAPS").[138] However, will these systems ever evolve to incorporate biometric identifiers?

In 1996, the Department of Transportation suggested a plan for a federalized driver's license that would include a biometric identifier.[139] Proponents of the plan stated that it would reduce the number of forged identity documents used by illegal immigrants to gain federal benefits.[140] In response to the proposal, the State of Georgia began placing fingerprints on Georgia driver's licenses in April 1996.[141] California, Colorado, Florida, and Hawaii already required fingerprints on their driver's licenses before the proposal was made.[142] Support for

---

to prove that they are U.S. citizens or have clearance to work in the United States. Sobel, *Demeaning*, *supra* note 133, at 325.

[135] Illegal Reform and Immigration Responsibility Act of 1996, Pub. L. No. 104-208, 110 Stat. 3009-546 to 3009-724 (1996). This statute required employees to show their employers identification to prove citizenship or government permission to work. Sobel, *Demeaning*, *supra* note 133, at 324.

[136] Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193, 110 Stat. 2105 (1996). This statute created a federal database to track all newly hired employees. The database recorded names, addresses, Social Security numbers, and wages of all employees hired after October 1, 1997. Sobel, *Demeaning*, *supra* note 133, at 324-25.

[137] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996). This statute required the development of a "unique health identifier" and a national electronic collection system for personal health care data. Sobel, *Demeaning*, *supra* note 133, at 325.

[138] FAA procedure dictates that airlines request identification from passengers before they are allowed to board. The FAA directive, which is the basis for this ID requirement, appears not to have been released. Sobel, *Demeaning*, *supra* note 133, at 325-326, 387 n. 27; *see also* Sobel, *Degradation*, *infra* note 139.

[139] Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37, 44 (2002) [hereinafter Sobel, *Degradation*].

[140] *Id.*

[141] *Id.*

[142] *Id.*

this type of national identification system has grown since the attacks of September 11, 2001.[143]

Supporters of a national identification system with biometric identifiers claim that it would be one of the best ways to prevent terrorists from operating under assumed names and to protect secured locations, such as airports.[144] Larry Ellison, CEO of Oracle Corporation, has proposed a national database that contains a combination of many types of biometrics including thumb prints, hand prints, and iris scans.[145] The proposed database would also contain information such as names, addresses, places of employment, amounts and sources of income, purchases, assets, and travel destinations.[146] Under Ellison's system, to gain entry into an airport, people would have to present a photo ID, put their thumb on a fingerprint scanner, and tell the guard what their social security number was.[147] Ellison's company, Oracle, has "already offered to provide the necessary software for free, and [] other companies would pitch in with hardware and support."[148]

Other supporters of a national identification system have claimed that it would "aid in fraud prevention..., catch 'deadbeat dads,' enable electoral reforms, allow quick background checks for those buying guns or other monitored items, and prevent illegal aliens from working in the United States."[149]

Critics of national identification cards, with or without biometric information, state that such a system would impact due process, freedom from unreasonable search, free expression, the right to employment, separation of powers, freedom of travel, and

---

[143] Sobel, *Demeaning*, *supra* note 133, at 332.

[144] *Id.* at 334.

[145] *Id.*

[146] *Id.*

[147] *Id.*

[148] *Id.* (citing Larry Ellison, Digital Ids Can Help Prevent Terrorism, WALL ST. J., Oct. 8, 2001 at A26).

[149] Daniel J. Steinbock, *National Identity Cards: Fourth and Fifth Amendment Issues*, 56 FLA. L. REV. 697, 702-703 (2004) (citing Committee on Authentication Technologies and Their Privacy Implications, National Research Council, *IDs-Not that Easy: Questions About Nationwide Identity Systems*, at 6 (Stephen T. Kent & Lynette I. Millet eds., 2002)).

federalism.[150] Sobel has stated that "the existence of databanks and identification schemes implies that society has a right to surveil its subjects and to define individual identities separate from the inherent nature of personhood."[151]

Those in Hong Kong have responded to the new national smart card system with an increased concern and awareness of privacy issues. Stephen Lau, Hong Kong's Privacy Commissioner at the time the smart card plan was unveiled, claimed that historically, Chinese people did not possess a strong concept of "privacy."[152] However, a recent survey conducted by the Privacy Commission showed that the Chinese people ranked privacy as their third most important priority, after unemployment and environmental protection, but before food hygiene and medical services.[153] Residents of Hong Kong worry that, although the government has said that it will be careful with biometric data, this data may find its way into the hands of the private sector.[154] However, the people of Hong Kong still think that the smart card is the best form of identification and use it for such.[155]

V. DNA DATABASES

The use of deoxyriboneuclic acid (DNA) in law enforcement has grown in recent years. DNA is extremely helpful in the identification of a criminal. All fifty states and the District of Columbia have implemented laws requiring convicted criminals to submit their DNA so that it may be stored in criminal databases.[156] The federal government has also enacted a statute authorizing a DNA databank.[157] These laws were heavily challenged during the year of 2004, and the

---

[150] Sobel, *Demeaning*, *supra* note 133, at 320.

[151] *Id.* at 322.

[152] Chung, *supra* note 119, at 446.

[153] *Id.* at 446-447.

[154] *Id.* at 447.

[155] *Id.*

[156] John P. Cronan, *The Next Frontier of Law Enforcement: A Proposal for Complete DNA Databanks*, 28 AM. J. CRIM. L. 119, 131-32 (2000).

[157] DNA Identification Act of 1994, Pub. L. No. 103-322, 108 Stat. 2068 (codified at U.S.C. § 14131-34).

vast majority were laws upheld.[158] But, would a federal law mandating a complete DNA database of the entire United States citizenry be justified and upheld?

A. DNA DATABASES IN THE CRIMINAL CONTEXT

For most people, DNA collection from criminals is a sensible extension of biometric technology. This system has its critics, however. Benajamin Keehn, a Boston public defender representing prisoners suing to avoid DNA collection, has said that DNA collection "amounts to an unconstitutional warrantless search on a national scale. It's a computer-age version of 'round up the usual suspects.'"[159] Others have agreed with him, and there have been many different challenges to DNA collection statutes, including challenges under the Fourth Amendment and the Fifth Amendment.

1. DNA COLLECTION CHALLENGES UNDER THE FOURTH AMENDMENT

The Fourth Amendment protects citizens from "unreasonable searches and seizures."[160] The courts have been divided on their approach to the DNA collection statutes. Some courts have found that the collection of DNA constituted a Fourth Amendment search, but upheld the search under a special needs test.[161] Other courts have denied that there was a Fourth Amendment search at all.[162] In yet

---

[158] *See* United States v. Kincade, 379 F.3d 813 (9th Cir. 2004) in which the court upheld California's DNA Analysis Backlog Elimination Act of 2000 under the 4th Amendment. *See also* Moss v. Johnson, 2:04-CV-0142, 2004 U.S. Dist. LEXIS 20049 (N.D. Tex. 2004) in which the court upheld Texas' DNA collection statute under the first amendment free exercise clause, the fourth amendment, the fifth amendment, the fourteenth amendment, and the eighth amendment.

[159] Cronan, *supra* note 156, at 142 (citing Richard Willing, *FBI Activates 50-State DNA Database Tuesday*, USA TODAY, Oct. 12,1998, at A1).

[160] U.S. CONST. amend. IV.

[161] *See* Green v. Berge (7th Cir. 2004), 354 F.3d 675 in which the Seventh Circuit held that the DNA collection of criminals was reasonable because it met the special needs test. The Court noted that "The DNA Act, while implicating the Fourth Amendment, is a reasonable search and seizure under the special needs exception to the Fourth Amendment's warrant requirement because the desire to build a DNA database goes beyond the ordinary law enforcement need."

[162] *See* Nicholas v. Goord, No. 01 Civ. 7891, 2004 U.S. Dist. LEXIS 11708 (S.D.N.Y. 2004). The New York District Court suggested that collection of DNA from a criminal may not constitute as a search under the Fourth Amendment.

another approach, others courts have upheld the statutes because the search was not considered unreasonable.[163]

2. DNA COLLECTION CHALLENGES BASED ON THE FIFTH AMENDMENT

The Fifth Amendment guarantees freedom from self-incrimination.[164] Some challengers of the DNA collection statutes argue that the mandatory collection of DNA violates this right against self-incrimination.[165] It has been said that any Fifth Amendment challenge to DNA testing must fail because DNA samples are not testimonial in nature.[166]

B. COMPLETE DNA DATABASES

Although criminal DNA databases are usually accepted and approved, DNA databases containing all people in the United States are more controversial. One supporter has proposed that DNA databases be expanded to contain every person in the country through three methods of DNA collection: (1) Collection at birth, (2) collection from new entrants into the country, and (3) continuing collection from certain classes of criminals.[167]

Opponents of universal DNA databases argue that this type of collection would violate the Fourth Amendment's protection against unwarranted and unreasonable searches. Others critics stated that the implementation of a universal DNA database would create a nation of suspects and dramatically change the relationship between the government and the citizenry.[168] Under this theory, the database

---

[163] *Id.* The New York District Court held that DNA collection of criminals was reasonable. The court balanced the search's intrusion on an individual's Fourth Amendment Rights against the government's interests in pursuing the search. The court considered the strength of the individual's privacy interest, the nature and scope of the intrusion, and the government interest at stake.

[164] U.S. CONST. amend. V.

[165] Lloyd v. Mechling, 848 A.2d 1094, 1096 (Pa. Commw. Ct. 2004).

[166] *See id.*

[167] Cronan, *supra* note 156, at 137-138.

[168] D.H. Kaye & Micheal E. Smith, *DNA Identification Databases: Legality, Legitimacy, and the Case for Population-Wide Coverage*, 2003 WIS. L. REV. 413, 446 (2003).

would create an "ethos of suspicion."[169] Another argument is that a universal database could never be implemented because the general public opposes it.[170] Finally, others challenge the expense of creating and maintaining such a system.[171]

Proponents of universal DNA databases state that a database of this type would lead to increased conviction rates, deterrence leading to a lower crime rate, and reduction of wrongful arrests.[172] This system could also decrease the number of missing persons.[173] Proponents also note that the current system is quite skewed because of the large number of felons who are black males.[174] If the general population were allowed to be sampled, this would clearly decrease the internal bias present in the current system.[175]

VI. CONCLUSION

As we head further into the new millennium, biometrics will undoubtedly become a part of everyday life. This will present new challenges to the legal system. Policy-makers will have to resolve the tension between regulating technology and allowing progress to be made. They will have to decide between identifying individuals for safety reasons and maintaining a person's right to anonymity. Although biometrics is science and technology on its surface, it is a tension between values and policies at its core. The regulation of biometrics will be an on-going debate for decades to come.

---

[169] *Id.*

[170] *Id.* at 440-441.

[171] *Id.* at 449.

[172] *See* Cronan, *supra* note 156.

[173] Kaye, *supra* note 168, at 450.

[174] *Id.* at 452-53.

[175] *Id.* at 454.